UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

ROSEMARY MOSQUEDA, individually and on behalf of all others similarly situated, Plaintiff, v. PROGRESS SOFTWARE CORPORATION and PENSION BENEFIT INFORMATION, LLC d/b/a PBI RESEARCH SERVICES Defendants.	Case No. 0:23-cv-02278 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Rosemary Mosqueda ("Plaintiff") individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to herself and on information and belief as to all other matters, brings this Class Action Complaint against Defendants Progress Software Corporation ("PSC") and Pension Benefit Information, LLC d/b/a PBI Research Services ("PBI" and collectively with PSC, "Defendants"), and in support thereof alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action on behalf of herself and all other individuals ("class members"), totaling more than 37 million people and 550 organizations, who had their sensitive personal identifiable information ("PII") and protected health information ("PHI")—as defined by the Health Insurance Portability and Accountability Act ("HIPPA")—accessed and hacked by malicious, unauthorized third parties that accessed

and removed the PII and PHI from Defendants' systems as early as May 27, 2023[1] (the "Data Breach").

2. Both Defendants tout the safety and security of their services on their websites. PSC advertises itself as an "experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely."[2] Likewise, the main page of PBI's website states: "Confidence Your Data is Secure: Protecting and securing your information is our highest priority. Our formalized security program follows industry-recognized security frameworks and undergoes an annual SSAE 18 SOC 2, Type II audit."[3]

3. PSC offers both solutions and products, including its file transfer service called MOVEit, which "provides secure collaboration and automated file transfers of sensitive data and advanced workflow automation capabilities without the need for scripting. Encryption and activity tracking enable compliance with regulations such as PCI, HIPAA and GDPR."[4]

4. Specifically, PSC describes MOVEit as a "managed file transfer software" that PSC claims is "leading secure Managed File Transfer (MFT) software used by thousands of organizations around the world to provide complete visibility and control over

[1] https://www.reuters.com/technology/hackers-use-flaw-popular-file-transfer-tool-steal-data-researchers-say-2023-06-02/ (last visited June 28, 2023); https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html
[2] https://www.progress.com/company (last visited August 1, 2023).
[3] https://www.pbinfo.com/ (last visited August 1, 2023).
[4] https://www.progress.com/moveit (last visited August 1, 2023).

file transfer activities. Whether deployed as-a-Service, in the Cloud, or on premises, MOVEit enables your organization to meet compliance standards, easily ensure the reliability of core business processes, and secure the transfer of sensitive data between partners, customers, users and systems."[5]

5. MOVEit is used by more than 1,700 software companies and 3.5 million users worldwide.[6]

6. PSC's wholly-owned subsidiary, Ipswitch, Inc. ("Ipswitch"), developed MOVEit along with other products that "enable small and medium sized business and enterprises to provide secure data sharing and ensure high-performance infrastructure" and was acquired by PSC in 2019.[7]

7. PSC's website states[8]:

> to comply with HIPAA, Progress operates secure computing environments in its corporate offices, development environments, and production cloud products. Each of these areas are equipped with security technologies, processes, and people needed to protect sensitive information. The Progress Internal Audit team audits use of security solutions and processes, evaluated by annual SOC2 assessments and validated by annual HIPAA audits. Copies of the SOC2 assessments and audit reports are available to our customers upon request. Progress corporate administration and human resources functions are also audited for HIPAA compliance on an annual basis.

[5] https://www.ipswitch.com/moveit?_ga=2.178322852.1251772019.1689781398-357640369.1688748444 (last visited August 1, 2023).
[6] https://www.jdsupra.com/legalnews/moveit-transfer-zero-day-vulnerability-9280864/#:~:text=With%20more%20than%201%2C700%20software,unidentified%20threat%20actor%20groups%20worldwide (last visited August 1, 2023).
[7] https://investors.progress.com/news-releases/news-release-details/progress-acquire-ipswitch-inc (last visited August 1, 2023).
[8] https://www.progress.com/legal/hipaa-compliance-faqs (last visited August 1, 2023).

8. PSC's website states that "within our Sites, you may be asked to give us personal or organizational information in order to purchase or receive information about a Progress Property. We may collect this information through different methods."[9]

9. PSC's website further states that "in some cases, end users of our customers may need to provide Sensitive Personal Information to our customer in order to make use of an application that uses our Product or SaaS Product and that Sensitive Personal Information may be stored or processed by us as a result. We process such Sensitive Personal Information in the role of a processor on behalf of a customer (and/or its affiliates) who is the responsible controller of the Sensitive Personal Information concerned."[10]

10. PSC's website explains[11]:

> the Personal Information collected by Progress Software may include, but is not necessarily limited to:
>
> - Contact information (such as your name, title, e-mail address, postal address, and telephone number);
> - Transactional information, including delivery details, including billing and delivery address where applicable;
> - User preferences;
> - IP address;
> - Financial/credit card and payment information (please see the "Third Party Payment Processor" section for more information);
> - Demographic information and geographic or geo-location information; and
> - Additional information as needed for our business and customer service purpose.

11. PBI is a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans, and one of the many companies that uses

[9] https://www.progress.com/legal/privacy-policy (last visited August 1, 2023).
[10] *Id.*
[11] *Id.*

PSC's MOVEit service to transfer large amounts of data in the ordinary course of its business and the service it provides to pension plans and other organizations.[12] For instance, the California Public Employees' Retirement System ("CalPERS") is one such pension plan that uses PBI's services and, in turn, PSC's MOVEit service. Following the Data Breach, CalPERS sent letters to its pension participants informing them of the Data Breach, which stated that it was caused by PBI's use of PSC's MOVEit service[13]:

> CalPERS was informed about a recent cybersecurity breach at our third-party vendor PBI Research Services/Berwyn Group ("PBI") involving their MOVEit Transfer Application, which is used by organizations worldwide. We use PBI's services to ensure accurate payments to retirees and beneficiaries and sent data to PBI in a secure, encrypted format …. Specifically, PBI provides services to … ensure that proper payments are made to retirees and beneficiaries …. PBI also validates information on inactive members who may soon be eligible for benefits. On June 6, 2023, PBI notified us that a previously unknown "zero-day" vulnerability in their MOVEit Transfer Application allowed our data to be downloaded by an unauthorized third party …. Personal information that was downloaded included: first and last name; date of birth; and Social Security number. It could have also included the names of former or current employers, spouses or domestic partners, and children. The information that was taken involves anyone who was receiving an ongoing monthly benefit payment as of this spring.

12. On or around May 31, 2023, PSC purportedly discovered a vulnerability in its MOVEit Transfer and MOVEit Cloud systems that "could lead to escalated privileges and potential unauthorized access." On or about that same day, PSC purportedly notified

[12] https://www.pbinfo.com/ (last visited August 1, 2023).
[13] https://www.calpers.ca.gov/page/home/pbi (last visited August 1, 2023).

all customers, and developed and released a security patch with 48 hours.[14] PSC assigned a severity rating of 9.8 out of 10 to this vulnerability.[15]

13. On or around June 9, 2023, PSC and its contracted cybersecurity firm, Huntress, uncovered additional vulnerabilities "distinct from the previously reported vulnerability shared on May 31, 2023."[16]

14. It has been reported that the Data Breach affecting PSC's MOVEit software is unique from most other recent data breaches because MOVEit is widely used, and the breach impacted both primary users of the software, as well as their contracted third parties that also use the software.[17]

15. It has been reported that the Data Breach was a ransomware attack conducted by a notorious ransomware group, C10p, which claims to have committed the Data Breach.[18]

16. C10p claims to have stolen PII and PHI information from over 550 organizations and 37 million individuals, including U.S. schools, U.S. public sector, and U.S. private sector.[19]

17. C10p is a well-known ransomware group, which "[has] been linked to FIN11, a financially-motivated cybercrime operation" and is "connected to both Russia

[14] https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability (last visited August 1, 2023).
[15] https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ (last visited August 1, 2023).
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*; https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html

and Ukraine and which is believed to be part of a larger umbrella operation known as TA505."[20]

18. It has been reported that C10p has requested unspecified ransom from the impacted organizations in exchange for C10p to abstain from releasing consumers' highly sensitive PII and PHI. As of July 19, 2023, C10p and its hacking of MOVEit has resulted in the theft of more than 37 million individuals' sensitive information.[21] Because the Data Breach was conducted by known, self-proclaimed ransomware hackers, Plaintiff's and class members' sensitive PII and PHI are irrefutably in the possession of known bad actors.

19. Defendants owed duties to Plaintiff and class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII and PHI against unauthorized access and disclosure. Defendants breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII and PHI entrusted to it from unauthorized access and disclosure.

20. As a result of Defendants' inadequate security and breach of its duties and obligations, the Data Breach occurred and Plaintiff's and class members' PII and PHI was accessed by, and disclosed to, an unauthorized third-party actor. This instant action seeks to remedy these failings and their consequences. Plaintiff thus brings this complaint on behalf of herself and all similarly situated individuals whose PII and/or PHI was exposed

[20] *Id.*
[21] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html

as a result of the Data Breach, which PSC learned of on or about May 27, 2023, but did not publicly disclose until May 31, 2023.

21. Plaintiff, on behalf of herself and all other class members, asserts claims for negligence, negligence per se, invasion of privacy, unjust enrichment, California Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq.*), California Customer Records Act (Cal. Civ. Code § 1798.80, *et seq.*), California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200, *et seq.*), and California Constitution, art. 1, § 1, and seeks declaratory and injunctive relief, monetary damages including punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

A. Plaintiff

22. Plaintiff is a resident and citizen of the state of California and resides in Sacramento, California.

23. Plaintiff received a letter from CalPERS dated June 22, 2023, confirming that her PII and PHI were impacted by the Data Breach and accessed by cybercriminals that accessed Defendants' systems:

> We are writing to inform you about a recent cybersecurity breach at our third-party provider, PBI Research Services/Berwyn Group ("PBI") involving the MOVEit Transfer application …. Your personal information that was downloaded included: full name, date of birth and Social Security number. It could have also included the names of your child or children.

24. Prior to retaining counsel for claims related to the Data Breach, Plaintiff spent at least an hour monitoring her accounts for fraudulent activity and identity theft. She

will continue to expend further time doing so in the days, weeks, and months following the filing of this complaint.

B. Defendant Progress Software Corporation

25. PSC is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803. PSC offers the service MOVEit, which experienced the Data Breach underlying Plaintiff's claims.

C. Defendant Pension Benefit Information, LLC d/b/a PBI Research Services

26. PBI is a for-profit Delaware corporation with its principal place of business at 333 S 7th Street, Suite 2400, Minneapolis, MN 55402. PBI uses PSC's MOVEit service in the regular course of its business acting as a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans.[22]

JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000) and is a class action in which one or more class members are citizens of states different from Defendants.

28. The Court has general personal jurisdiction over Defendant PBI because it maintains its headquarters and principal place of business in this judicial District (i.e., in

[22] https://www.pbinfo.com/ (last visited August 1, 2023).

Minneapolis, Minnesota). This Court has general personal jurisdiction over Defendant PSC because PSC is registered to conduct business in Minnesota and has a registered office address in Roseville, Minnesota. Defendants have minimum contacts with Minnesota because they conduct substantial business in the state.

29. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391 because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in Minnesota, Defendants maintain physical offices and places of business in this District, and because Defendants conduct a substantial part of their business within this District.

FACTUAL ALLEGATIONS

A. Overview of Defendants

30. PSC advertises itself as "the experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely."[23]

31. PSC offers both solutions and products, including MOVEit, which "provides secure collaboration and automated file transfers of sensitive data and advanced workflow automation capabilities without the need for scripting. Encryption and activity tracking enable compliance with regulations such as PCI, HIPAA and GDPR."[24]

[23] https://www.progress.com/company (last visited August 1, 2023).
[24] https://www.progress.com/moveit (last visited August 1, 2023).

32. MOVEit is a "managed file transfer software" that PSC claims is "leading secure Managed File Transfer (MFT) software used by thousands of organizations around the world to provide complete visibility and control over file transfer activities. Whether deployed as-a-Service, in the Cloud, or on premises, MOVEit enables your organization to meet compliance standards, easily ensure the reliability of core business processes, and secure the transfer of sensitive data between partners, customers, users and systems."[25]

33. PSC claims MOVEit has "flexible architecture makes it easy to choose the exact capabilities that match your organization's specific needs,"[26] which include three modules:

- **MOVEit Cloud** – "MOVEit Cloud enables the consolidation of all file transfer activities to one system to ensure better management control over core business processes. A trusted and proven SaaS solution, it provides full security, reliability and compliance with the convenience of a cloud-based service. It provides the security, centralized access controls, file encryption and activity tracking needed to ensure operational reliability and compliance with SLAs, internal governance and regulatory requirements like PCI, HIPAA, CCPA/CPRA and GDPR."[27]
- **MOVEit Transfer** – "MOVEit Transfer provides the same award-winning capabilities of MOVEit Cloud in an on-premises solution. Ensure management

[25] https://www.ipswitch.com/moveit?_ga=2.178322852.1251772019.1689781398-357640369.1688748444 (last visited August 1, 2023).
[26] *Id.*
[27] *Id.*

and control over your business-critical file transfers by consolidating them all on one system. Leverage MOVEit Transfer's file encryption, security, activity tracking tamper-evident logging, and centralized access controls to meet your operational requirements. Reliably and easily comply with SLAs, internal governance requirements and regulations like PCI, HIPAA, CCPA/CPRA and GDPR."[28]

- **MOVEit Automation** – "MOVEit Automation works with MOVEit Cloud, MOVEit Transfer to let admins and authorized users easily create file-based tasks without programming. It automates and controls access to file transfer resources, minimizes workloads and reduces errors while mitigating the risk of data loss. You get a reliable, secure means of sharing business data with an audit trail and visibility into all file transfer activities."[29]

34. MOVEit is used by more than 1,700 software companies and 3.5 million users worldwide.[30]

35. Ipswitch developed MOVEit along with other products that "enable small and medium sized business and enterprises to provide secure data sharing and ensure high-performance infrastructure" and was acquired by PSC in 2019.[31]

---

[28] *Id*.
[29] *Id*.
[30] https://www.jdsupra.com/legalnews/moveit-transfer-zero-day-vulnerability-9280864/#:~:text=With%20more%20than%201%2C700%20software,unidentified%20threat%20actor%20groups%20worldwide (last visited August 1, 2023).
[31] https://investors.progress.com/news-releases/news-release-details/progress-acquire-ipswitch-inc (last visited August 1, 2023).

36. PSC's website assures viewers that its MOVEit service is safe and secure: "[PSC] is the experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, **then manage it all safely and securely**."[32]

37. PSC's website states that its MOVEit product allows for the secure transfer of sensitive information, in particular, in compliance with HIPAA and industry privacy standards: "[MOVEit] provides **secure** collaboration and automated file transfers of **sensitive data** and advanced workflow automation capabilities without the need for scripting. Encryption and activity tracking **enable compliance with regulations such as PCI, HIPAA and GDPR**."[33]

38. Likewise, PSC advertises its MOVEit product as a way to "**securely share files** across the enterprise and globally" and "transfer[s] **sensitive information securely**" while "let[ting] end users collaborate securely."[34]

[32] https://www.progress.com/company (last visited August 1, 2023).
[33] https://www.progress.com/moveit (last visited August 2, 2023).
[34] *Id.*

Everyone's demanding security and compliance, but nobody's giving you the resources to make it happen.

The federal government passes sweeping legislation like HIPAA and HITECH. State governments follow suit with mandates such as the Standards for The Protection of Personal Information of Residents of the Commonwealth (applicable in Massachusetts). The regulators oversee your organization as they enforce the laws. And your organization's leadership team promises to comply. But then...an over-eager end user who insists on an "easy, fast" workaround makes a totally avoidable PICNIC (Problem in Chair Not In Computer) mistake that leads to file security being compromised.

You're the one who's asked to fix the problem. And what a problem it is: If you can't produce the right files at the right time, or if you can't prove they were properly protected, your organization could be subject to millions of dollars in government fines and penalties, a battered reputation in the healthcare community, and a loss of trust by medical professionals, patients, and the public at large.

39. PSC advertises its MOVEit product as a secure Managed File Transfer (MFT) system that allows users to transfer data securely, in complete fulfillment of their compliance requirements[35]:

> [MOVEit] allows you to meet your growing (and increasingly complex) file transfer needs. It can be delivered to your doorstep neatly and simply. And **it enables you to transfer files reliably and securely**, meet all your all-important compliance requirements, eliminate manual workflows, and provide end users with an IT-approved solution for sending files. MFT also guarantees you visibility and control over all file transfer activities, enables you to confidently meet your SLAs, and provides you with easy implementation/on-boarding.

40. PSC's website states further:

[35] https://www.ipswitch.com/resources/best-practices/secure-healthcare-file-transfer (last visited August 2, 2023).

Specifically, with MOVEit from Progress you'll receive four vital benefits that are unavailable with the all-too-common array of legacy systems:

- Connectivity ensures that end users can access the system via mobile devices, email, or a web browser. IT retains control yet workers maintain high levels of productivity through easy-to-use, flexible access.
- Administration so that you can easily set up, control, and manage your organizational file transfers, provision users/accounts easily, and onboard partners and control access.
- Automation to make sure that files route appropriately according to key business processes and they integrate into other applications for scheduling and routing.
- Reporting for enterprise visibility and control, compliance and governance and to easily provide reports for auditing and regulatory inquiries.

41. In its whitepaper "7 Steps to Compliance with Data Protection Laws," PSC acknowledges that organizations that transfer and store PII and PHI face serious threats to ensuring the integrity of that information[36]:

> Stolen Personal Information (PI) drives a thriving black market for cybercriminals on a global basis. Since PI includes any data which can be used to identify an individual, every organization that collects data such as passwords, credit card data, health information and addresses is a potential target for cybercriminals. Not surprisingly, since 2013 data breaches have accounted for nearly 6 billion stolen data records globally. Also not surprisingly, governments around the world have responded with increasingly strict regulations regarding the collection, retention, processing and sharing of PI. Failure to comply with these regulations can result in severe fines.

42. PSC is well aware of its legal obligations and industry standards-imposing duties to protect consumers' sensitive PII and PHI because in this white paper, PSC details seven best practices for ensuring data integrity and meeting compliance with data

[36] This whitepaper can be accessed through the following link: https://www.ipswitch.com/resources/whitepapers-ebooks/7-steps-to-data-protection-law-compliance (last visited August 2, 2023).

protection laws:

AUTOMATION

Commonly used file transfer workflows should be automated to mitigate against the introduction of human error that might result in data loss. Your file transfer tools should support functions such as automatic forwarding, error correction, and confirmation of receipt for all data transfers.

CONTROL AND VISIBILITY

Control and visibility of transfer activities are important security requirements and essential for validating compliance. Your tools should enable central visibility, control and prior authorization of all file transfers. Logs should be kept in a tamper-evident database to assure the integrity of audit trails.

INFORMATION SECURITY

Your technology, tools or processes should ensure file integrity checks, data deletion after receipt, and non-repudiation (the sender and receiver are both authorized and authenticated to access the data). They should provide an automated audit trail that tracks integrity, delivery and authentication

AUTHENTICATION

Effective authentication of users and administrators is an essential control. Your file transfer systems should accommodate an array of access control mechanisms, including integration with central user directories, role-based access control and single sign-on as well as multi-factor authentication.

CRYPTOGRAPHY

Encryption algorithms have a limited shelf life. Compliance standards often do not allow the use of compromised systems. It is essential that your systems employ strong, state-of-the-art cryptographic mechanisms and enable secure selection, distribution and protection of encryption keys.

SECURE ARCHITECTURE

Your systems architecture should integrate with existing security infrastructures and applications. The systems should also either ensure that there is no unencrypted data within the DMZ or provide for DMZ termination of inbound requests for authentication and data transfer with a gateway proxy server.

FAILOVER

A key requirement of many data protection regulations is secure business continuity. This requirement is meant to safeguard the confidentiality, integrity and availability of file transfers, at all stages throughout any failures, disasters or outages. Automatic, secure failover is essential to ensure that file transfers are either successful or continuously restarted until complete.

43. In this whitepaper, PSC emphasizes the security of MOVEit, and advertises it as a MFT system that can address "each of the seven core best-practices for compliance

with data protection regulations"[37]:

MOVEit Compliance Features

MOVEit® is a Managed File Transfer system that lets you manage, view, secure, and control the exchange of sensitive data with external parties to assure compliance with data protection regulations. The table below shows how MOVEit addresses each of the seven core best-practices for compliance with data protection regulations.

Security Requirement	MOVEit Control
Compliance	MOVEit helps ensure that file transfers are secured, data is protected at all times, and records of transfers are secured in tamper-proof audit trails for legally required periods prior to assured destruction.
Communications Security	MOVEit enables central visibility, control and prior authorization of all file transfers, as well as encryption, traceability and non-repudiation of transfers, including secure audit trails of significant events. MOVEit is architected to integrate with existing security infrastructure, policies, and applications, ensuring there is no unencrypted data in the DMZ and eliminating any requirement for external access.
Information Security Policies	MOVEit encrypts files at rest and in transit, provides non-repudiation and file integrity checks. Ipswitch provides email, web, mobile access and desktop clients which, when used with MOVEit provide compliant file transfer access to all users.
Access Control	MOVEit offers a choice of authentication mechanisms, including integrations with existing systems, and a rich set of features to support user access management, including blacklists and whitelists, and tools to help administrators select the most appropriate settings to meet security policies.
Cryptography	MOVEit employs strong cryptographic mechanisms and secure selection, distribution and protection of encryption and decryption keys, consistent with international legal and regulatory requirements.
Physical & Environmental Security	MOVEit provides flexibility in implementation to ensure adherence to local physical security requirements.
Business Continuity Security	MOVEit safeguards the confidentiality, integrity and availability of file transfers at all stages throughout any failures, disasters or outages. Ipswitch Failover can assure uninterrupted file transfer processing.

44. PSC's Privacy Policy posted on its website notes that PSC is committed to protecting the privacy of individuals[38]:

[37] *Id.*

[38] https://www.progress.com/legal/privacy-policy (last visited August 2, 2023).

> Progress Software Corporation, together with its subsidiaries and affiliates, ("Progress", "we", "us", "our" or the "Company") is committed to protecting the privacy of individuals who visit the Company's web sites, individuals who register to use our services, and individuals who register to attend the Company's corporate events. This Privacy Policy (the "Policy") describes Progress' privacy practices in relation to the use of the Company's web sites and the related applications, services, and programs offered by the Company, as well as individuals' choices regarding use, access and correction of personal information.

45. PSC's Privacy Policy promises consumers that it has systems and processes in place to ensure the security and privacy of their sensitive PII and PHI, in compliance with governing law and industry standards[39]:

> **Our Security Practices**
>
> Progress employs industry standard security measures to ensure the security of information. However, the security of information transmitted through the Internet can never be guaranteed. Progress is not responsible for any interception or interruption of any communications through the internet or for changes to or losses of information. Users of our Sites are responsible for maintaining the security of any password, user ID, or other form of authentication involved in obtaining access to password protected or secure areas of any of our websites. To protect you and your information, Progress may suspend your use of a website, without notice, pending an investigation, if any breach of security is suspected. Access to and use of password protected and/or secure area of any Progress Software site is restricted to authorized users only. Unauthorized access to such areas is prohibited and may lead to criminal prosecution.
>
> We have put in place physical, electronic, and managerial procedures designed to help prevent unauthorized access, to maintain data security, and to use correctly the Information we collect online. These safeguards vary based on the sensitivity of the information that we collect and store. We also use administrative, technical, and physical security measures to help protect your personal information. While we have taken reasonable steps to secure the personal information you provide to us, please be aware that despite our efforts, no security measures are perfect or impenetrable, and no method of data transmission can be guaranteed against any interception or other type of misuse. Any information disclosed online is vulnerable to interception and misuse by unauthorized parties. Therefore, we cannot guarantee complete security if you provide personal information.

[39] https://www.progress.com/legal/privacy-policy (last visited August 2, 2023).

46. PSC's Privacy Policy assures consumers that it will not share their sensitive information—which necessarily includes by letting a data breach access it—without first obtaining the consumers' written consent:

> Notwithstanding the above, if we ever need to handle Sensitive Personal Information about you, we will ask your consent to do so. Once given, such consent may be withdrawn at any time. We will not handle any Sensitive Personal Information that we are not permitted by you to handle, or that you have not provided us with. Any Personal Information about you that we handle will only be accessible by those Progress personnel who have a reason to do so.[40]

> With your consent (when required), we may use and share the Personal Information we collect to: provide, support and improve the Progress Properties; deliver correspondence, communications, or services, such as newsletters, events, training, or software that you request or purchase; process orders; confirm licensing compliance; solicit your feedback; and inform you about the Company and the products and services of our distributors, resellers and promotional partners.[41]

47. PSC acknowledges that some of its products are Covered Entities under HIPAA and thus are required to entire into Business Associate Agreements.[42]

48. PSC acknowledges that it has a legal duty to safeguard PII and PHI under HIPAA and takes the following steps to meet its legal obligations[43]:

> To comply with HIPAA, Progress operates secure computing environments in its corporate offices, development environments, and production cloud products. Each of these areas are equipped with security technologies, processes, and people needed to protect sensitive information. The Progress Internal Audit team audits use of security solutions and processes, evaluated by annual SOC2 assessments and validated by annual HIPAA audits. Copies of the SOC2 assessments and audit reports are available to our customers

[40] *Id.*
[41] *Id.*
[42] https://www.progress.com/legal/hipaa-compliance-faqs (last visited August 2, 2023).
[43] *Id.*

upon request. Progress corporate administration and human resources functions are also audited for HIPAA compliance on an annual basis.

49. PSC further assures consumers that as an additional measure to ensure data integrity, it implements and maintains an Executive Security Committee, which conducts annual audits of its systems, among other things, to identify vulnerabilities:[44]

Summary

Progress Software operates an Executive Security Committee which has directed that a security program and supporting policy framework be operated to protect the security interests of company infrastructure, the software it produces, and customer solutions it operates. The company information security program is responsible for protecting the confidentiality, integrity, and availability of information handled by company technology systems and outwardly facing technology products. It is established that this function will identify, assess, monitor, and remediate security issues in a manner that keeps risks under control and within company and customer appetite. The program is operated according to applicable laws, regulations, and industry best practices. The function shall leverage colleagues from across the company to effectively manage risk, and efforts remain transparent to leadership. The following program components underpin the Progress' Information Security Program.

Company Information Security Strategy

On an annual basis, company information security officers present to management a revised corporate information security strategy aimed at protecting the confidentiality, integrity, and availability of company systems and customer facing products. Throughout the course of a given year risks are identified and tracked, existing information Security solutions are monitored, and new Security Technologies are researched. These ingredients converge on an annual basis into a strategic security plan that governs corporate information security strategy and product security related practices. These plans then influence initiatives, projects, policies and procedures across the company.

[44] https://www.progress.com/security/information-security-program-whitepaper (last visited August 2, 2023).

50. PSC's security policy is comprised of "a family of Information Security Policy documents that take the form of policies, standards, and procedural guidelines. Each of these types of document are published inside of progress to shape employee behaviors, maintain the security of our environment, and the security of our products. Such documents are kept in an electronic policy binder and made available to all employees."[45]

51. Likewise, PSC's security policy is targeted at its products to prevent vulnerabilities from being exploited:[46]

Product Security

All software products at progress are developed a via the use of modern methodologies, techniques, technologies, and processes. Our software development life cycles employ Agile methodologies while including numerous waves of security planning and testing. These include security requirements planning, security design planning, code level security scanning, vulnerability scanning, and penetration testing.

Threat and Vulnerability Management

Ongoing threat and vulnerability management activities performed on all corporate assets and customer facing product environments. These activities include monitoring of key government and media outlets to stay apprised of emerging security issues, vulnerability scanning of internal and external systems, penetration testing of products and corporate environments.

52. Similar to PSC, PBI's website also promises consumers that it has robust systems and processes in place to protect and secure their sensitive information:

[45] *Id.*
[46] *Id.*

pbi

Protecting and securing the information of our clients and our company is of critical importance to PBI. We recognize that all relationships with current and prospective clients are based upon integrity and trust, and we take our role as custodians of confidential information very seriously.

PBI uses a multi-layered approach to protect data securely that includes, but is not limited to the following: implementing secure development practices, including annual training for our IT team, real time scanning of code changes for vulnerabilities, web application firewalls, n-tier application architecture, required security awareness training program for all employees at onboarding and on a regular basis, data loss prevention tools to alert and block transfers of sensitive data, and a consolidated SIEM solution that correlates alerts and events across multiple environments. PBI's data security team manages this multi-layered security architecture by performing over 30 security reviews of quarterly audit checks to test compliance against security policies.

PBI's formalized security program follows the industry-recognized security policy frameworks from the National Institute of Science & Technology (NIST) SP 800-53 and NIST Cybersecurity Framework.

SOC2 Audit and Third-party Security Testing

PBI undergoes an annual SSAE 18 SOC 2, Type II audit by an independent third-party to audit our controls over data confidentiality, integrity, security, and availability.

PBI regularly uses third parties to test and audit our security controls. We conduct monthly and quarterly vulnerability assessments and penetration tests of PBI's internal and external network and application security, and conduct annual application penetration tests.

53. PBI's website also tells consumers that it has systems and process in place to ensure the privacy of their sensitive information obtained over the internet and to prevent identity theft:

> **9. ONLINE PRIVACY**
>
> PBI strives to protect the privacy of personally identifiable information obtained over the Internet and strives to apply the Principles and evolving standards to the online environment.
>
> **10. IDENTITY THEFT**
>
> PBI strives to prevent the acquisition of information from our products and services for improper purposes, such as identity theft. PBI believes in the importance of notifying individuals who may have had their sensitive personally identifiable information acquired by an unauthorized individual, as appropriate.

54. Furthermore, PBI acknowledges that it has a duty to safegaurd Plaintiff's and class members' sensitive PII and PHI because, *inter alia*, PBI's website tells consumers that it has systems in place to protect consumers' sensitive information, and routinely audits those systems to ensure they are compliant with federal regulations and other legislation— as well as industry standards and practices— governing data privacy:

> **8. ACCOUNTABILITY**
>
> PBI supports accountability of information industry standards and practices, responsible and effective federal regulation of the data industry, and legislation governing the practices of all data providers. PBI also supports industry oversight and active engagement with the privacy community. PBI believes that strong privacy and information security protections are vital for an effective and trusted data industry.

11. COMPLIANCE

PBI will obtain assessments from an independent auditor, who uses procedures and standards generally accepted in the profession to assess PBI's controls relevant to security, availability, and confidentiality, as appropriate.

55. Discovery will show that through their provision of the foregoing services, PSC and PBI obtain possession of customers'—including Plaintiff's and class members'—highly sensitive PII and PHI. Thus, in the regular course of their businesses, Defendants collect and/or maintain the PII and PHI of consumers such as Plaintiff and class members. Upon information and belief, that information ordinarily includes: (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) driver's license numbers or other state-issued ID numbers, (4) insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (5) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); (6) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by the provider); and (7) information of any parent, guardian, or guarantor. Defendants store this information digitally in the regular course of business.

56. As evidenced by, *inter alia*, their receipt of the notice informing them that their PII and PHI were compromised in the Data Breach, Plaintiff's and class members'

PII and/or PHI was transferred using PSC's MOVEit service and/or they otherwise entrusted to Defendants their PII and/or PHI, from which Defendants profited.

57. Yet, contrary to Defendants' website representations—by virtue of Defendants' admissions that they experienced the Data Breach which revealed the PII and PHI of more than 37 million individuals—Defendants did not have adequate measures in place to protect and maintain sensitive PII and PHI entrusted to it.[47] Instead, Defendants' websites wholly fail to disclose the truth: that Defendants lack sufficient processes to protect the PII and PHI that is entrusted to them.

B. The Data Breach

58. On or around May 31, 2023, PSC reported a vulnerability in its MOVEit Transfer and MOVEit Cloud systems that it said "could lead to escalated privileges and potential unauthorized access." On or about that same day, PSC purportedly notified all customers, and assigned a severity rating of 9.8 out of 10 to this vulnerability.

59. On or around June 9, 2023, PSC and its contracted cybersecurity firm, Huntress, uncovered additional vulnerabilities "district from the previously reported vulnerability shared on May 31, 2023."

60. It has been reported by organizations using MOVEit software that were affected by the breach that PII and PHI were stolen, including name, address, SSN, birthdate, height, eye color, driver's license number, vehicle registration information, handicap placard information, clinical information, demographic information, and

[47] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html

financial health information (such as insurance billing information), among others.[48] Upon information and belief, the compromised information includes sensitive medical records and information related to health care and visits.

61. On or about mid-July 2023, PBI sent notice of the Data Breach to class members stating as follows[49]:

> On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review on June 16, 2023, and confirmed that information concerning a limited number of consumers was among the records involved in this incident. For instance, the California Public Employees' Retirement System ("CalPERS") is one such pension plan that uses PBI's services and, in turn, PSC's MOVEit service.

Likewise, companies that utilize PBI's services also sent notice of the Data Breach to class members, such as the excerpt below from the notice CalPERS sent to its pension participants[50]:

> CalPERS was informed about a recent cybersecurity breach at our third-party vendor PBI Research Services/Berwyn Group ("PBI") involving their MOVEit Transfer Application, which is used by organizations worldwide. We use PBI's services to ensure accurate payments to retirees and beneficiaries and sent data to PBI in a secure, encrypted format …. Specifically, PBI provides services to … ensure that proper payments are

[48] https://www.expresslane.org/alerts/ (last visited August 2, 2023).
[49] https://apps.web.maine.gov/online/aeviewer/ME/40/a98d9ae9-b898-4aaa-8dde-de04551aaedb/af45f431-a61c-4c76-9d70-f31ab3236aa7/document.html (last visited August 2, 2023).
[50] https://www.calpers.ca.gov/page/home/pbi (last visited August 1, 2023).

> made to retirees and beneficiaries …. PBI also validates information on inactive members who may soon be eligible for benefits. On June 6, 2023, PBI notified us that a previously unknown "zero-day" vulnerability in their MOVEit Transfer Application allowed our data to be downloaded by an unauthorized third party …. Personal information that was downloaded included: first and last name; date of birth; and Social Security number. It could have also included the names of former or current employers, spouses or domestic partners, and children. The information that was taken involves anyone who was receiving an ongoing monthly benefit payment as of this spring.

62. Thus, the Data Breach resulted from Defendants' failure to adequately protect and safeguard the highly sensitive PII and PHI entrusted to them.

63. As noted above, it is believed that the Data Breach was a ransomware attack conducted by C10p, which itself claims to have committed the Data Breach.[51]

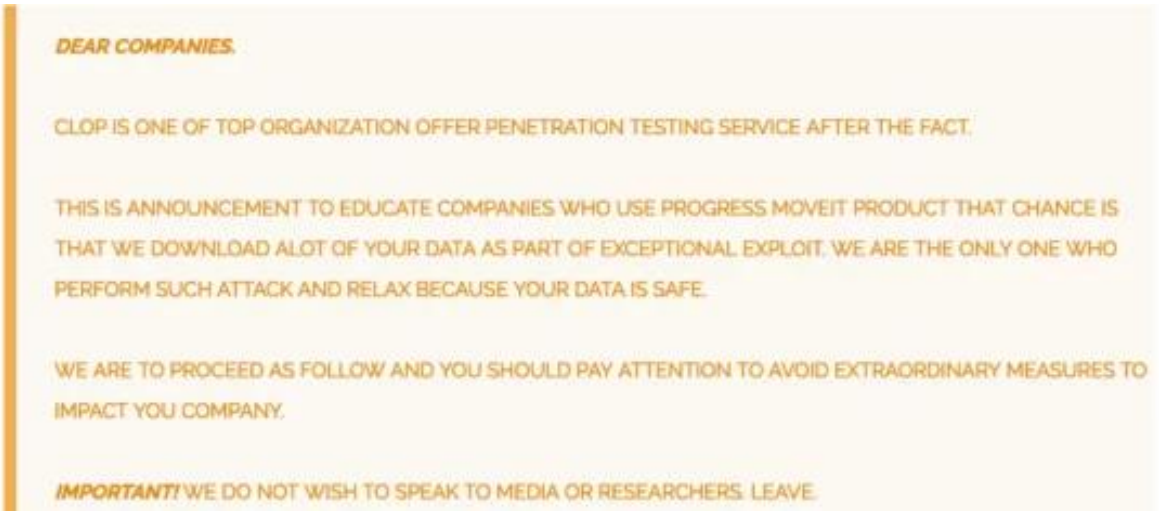
64. Through its hack of PSC's MOVEit service, C10p claims to have stolen PII and PHI information from over 550 organizations and 37 million individuals, including U.S. schools, the U.S. public sector, and the U.S. private sector.[52] C10p is a well-known ransomware group, which "[has] been linked to FIN11, a financially-motivated cybercrime operation" and is "connected to both Russia and Ukraine and which is believed to be part of a larger umbrella operation known as TA505."[53]

65. It has been reported that C10p has requested unspecified ransom from organizations impacted by the MOVEit Data Breach in exchange for C10p to abstain from releasing consumers' highly sensitive PII and PHI. As of July 19, 2023, C10p and its

[51] https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ (last visited August 2, 2023).
[52] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html
[53] *Id.*

hacking of MOVEit has resulted in the theft of more than 37 million individuals' sensitive information.[54] Because the Data Breach was conducted by known, self-proclaimed ransomware hackers, Plaintiff's and class members' sensitive PII and PHI are irrefutably in the possession of bad actors.

66. C10p posted a statement on its website demanding ransom from all companies impacted by the PSC MOVEit Data Breach, stating that if they refused to pay the ransom, C10p would post the sensitive PII and PHI stolen from Defendants' systems on the dark web[55]:



DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

[54] https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html
[55] *See supra* n.46.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

67. Because the Data Breach was conducted by known, self-proclaimed ransomware cybercriminals, Plaintiff's and class members' sensitive PII and PHI are irrefutably in the possession of known bad actors. Furthermore, Plaintiff's and class members' PII and PHI are already listed for sale on the dark web, which places them at imminent risk that their data will be misused.

68. As explicitly acknowledged and stated on their own websites, Defendants owed duties to Plaintiff and class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII and PHI against unauthorized access and disclosure, and to promptly notify individuals of any breach

involving their information. Defendants breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect PII and PHI from unauthorized access and disclosure.

C. Defendants Knew that Criminals Target PII and PHI

69. At all relevant times, Defendants knew, or should have known, the PII and PHI of individuals whose information was transferred using MOVEit—such as Plaintiff and all other class members—were targets for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and class members' information from cyber-attacks that Defendants should have anticipated and guarded against.

70. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were 758 medical data breaches in 2020 with over 40 million patient records exposed.[56] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[57]

[56] Protenus, *2021 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2021-breach-barometer (last accessed Nov. 15, 2021).
[57] Protenus, *2020 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2020-breach-barometer (last accessed Nov. 15, 2021).

71. PII and PHI are valuable property rights.[58] The value of this information as a commodity is measurable.[59] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[60] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[61] It is so valuable to identity thieves that once PII or PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

72. As a result of the real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII, PHI, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

---

[58] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data

[59] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[60] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[61] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

73. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[62] A cyber-criminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[63] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[64]

74. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[65] According to a report released by the FBI's Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[66]

---

[62] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[63] *Id.*

[64] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

[65] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[66] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

75. Criminals can use stolen PII and PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[67] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[68]

76. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[69]

77. Given these facts, any company that transacts business with a consumer and then compromises the privacy of that consumer's PII or PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

D. Theft of PII and PHI Has Grave and Lasting Consequences for Victims

78. Theft of PII and PHI is serious. The FTC warns consumers that identity thieves use PII and PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[70]

---

[67] *What Happens to Stolen Healthcare Data*, *supra* at n.10.
[68] *Id.*
[69] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.
[70] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE

79. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[71] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[72]

80. With access to an individual's PII or PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's

---

COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 15, 2021).

[71] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[72] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[73]

81. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[74]

82. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new SSN, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

83. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[75]

84. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical

---

[73] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Nov. 15, 2021).
[74] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Nov. 15, 2021).
[75] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

records that can plague victims' medical and financial lives for years."[76] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[77] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII and PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[78] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[79]

85. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought or received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their

[76] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf
[77] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.14.
[78] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Nov. 15, 2021).
[79] *Id*.

medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgages or other loans and may experience other financial impacts.

- Phantom medical debt collection based on medical billing or other identity information.

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[80]

86. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for a consumer to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[81]

87. It is within this harsh and dangerous reality that Plaintiff and all other class members must now live with the knowledge that their PII and PHI are forever in cyberspace and were taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

E. Damages Sustained by Plaintiff and the Other Class Members

[80] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 24.
[81] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

88. Plaintiff and all other class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—a risk that justifies expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the confidentiality of their PII and PHI; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

CLASS ALLEGATIONS

89. Plaintiff brings this action on behalf of herself and the following classes:

> Nationwide Class: All residents of the United States whose PHI and/or PII was compromised as a result of the Data Breach.
>
> California Subclass: All residents of California whose PHI and/or PII was compromised as a result of the Data Breach.

The foregoing classes are referred to herein, collectively, as the "Class." Excluded from the Class are: (1) the judges presiding over the action, Class Counsel, and members of their families; (2) the Defendants, their subsidiaries, parent companies, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

90. **Numerosity**: Class members are so numerous that their individual joinder is impracticable, as the proposed Class includes at least 37 million members who are geographically dispersed.

91. **Typicality**: Plaintiff's claims are typical of class members' claims. Plaintiff and all class members were injured through Defendants' uniform misconduct, and Plaintiff's claims are identical to the claims of the class members she seeks to represent.

92. **Adequacy**: Plaintiff's interests are aligned with the Class she seeks to represent and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and her counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiff and undersigned counsel.

93. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other class members' claims. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress Defendants' wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and

provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

94. **Commonality and Predominance:** The following questions common to all class members predominate over any potential questions affecting individual class members:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and class members' PII and PHI from unauthorized access and disclosure;

b. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and class members' PII and PHI;

c. Whether Defendants breached their duties to protect Plaintiff's and class members' PII and PHI;

d. Whether Defendants violated the statutes alleged herein;

e. Whether Plaintiff and all other class members are entitled to damages and the measure of such damages and relief.

95. Given that Defendants engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the California Subclass)

96. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

97. Defendants owed duties to Plaintiff and all other class members to exercise reasonable care in safeguarding and protecting their PII and PHI in Defendants' possession, custody, or control.

98. Defendants knew the risks of collecting and storing Plaintiff's and all other class members' PII and PHI and the importance of maintaining secure systems. Defendants knew of the many data breaches that targeted healthcare providers in recent years.

99. Given the nature of Defendants' businesses, the sensitivity and value of the PII and PHI it maintains, and the resources at its disposal, Defendants should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

100. Defendants breached their duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII and PHI entrusted to them—including Plaintiff's and class members' PII and PHI.

101. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and class members' PII and PHI to unauthorized individuals.

102. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and class members, their PII and PHI would not have been compromised.

103. As a result of Defendants' above-described wrongful actions, inactions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other class members have suffered, and will continue to suffer, economic damages and other injuries and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—a risk that justifies expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the confidentiality of their PII and PHI; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the California Subclass)

104. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

105. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

106. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure PII and PHI.

107. Defendants violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other class members' PII and PHI and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI they obtain and store, and the foreseeable consequences of a data breach involving PII and PHI including, specifically, the substantial damages that would result to Plaintiff and the other class members.

108. Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitute negligence per se.

109. Plaintiff and class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

110. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

111. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII and PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and class members' PII and PHI to unauthorized individuals.

112. The injury and harm that Plaintiff and the other class members suffered was the direct and proximate result of Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII and PHI; (iii) breach of the confidentiality of their PII and PHI; (iv) deprivation of the value of their PII and PHI, for which there is a well-established national and international market; and/or (v) lost time and

money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT III
INVASION OF PRIVACY
(INTRUSION UPON SECLUSION)
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the California Subclass)

113. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

114. The State of California recognizes the tort of Invasion of Privacy.

115. Plaintiff and class members had a reasonable expectation of privacy in the PII and PHI that Defendants failed to safeguard and allowed to be accessed by way of the Data Breach.

116. Defendants' conduct as alleged above intruded upon Plaintiff's and class members' seclusion under common law.

117. By intentionally and/or knowingly failing to keep Plaintiff's and class members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiff's and class members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and class members' private affairs in a manner that identifies Plaintiff and class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and class members,

which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and class members.

118. Defendants knew that an ordinary person in Plaintiff's and a class member's position would consider Defendants' intentional actions highly offensive and objectionable.

119. Defendants invaded Plaintiff and class members' right to privacy and intruded into Plaintiff's and class members' seclusion by intentionally failing to safeguard, misusing, and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

120. Defendants intentionally concealed from Plaintiff and class members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

121. As a proximate result of such intentional misuse and disclosures, Plaintiff's and class members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendants' conduct, amounting to a substantial and serious invasion of Plaintiff's and class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

122. In failing to protect Plaintiff's and class members' PII, and in intentionally misusing and/or disclosing their PII, Defendants acted with intentional malice and

oppression and in conscious disregard of Plaintiff's and class members' rights to have such information kept confidential and private.

123. As a direct and proximate result of the foregoing conduct, Plaintiff seeks an award of damages on behalf of herself and the Class.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the California Subclass)

124. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

125. Plaintiff and class members have both a legal and equitable interest in their PHI and PII that was collected by, stored by, and maintained by Defendants—thus conferring a benefit upon Defendants—that was ultimately compromised by the Data Breach.

126. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and class members. Defendants also benefitted from the receipt of Plaintiff's and class members' PHI and PII.

127. As a result of Defendants' failure to safeguard and protect PII and PHI, Plaintiff and class members suffered actual damages.

128. Defendants should not be permitted to retain the benefit belonging to Plaintiff and class members because Defendants failed to adequately implement the data privacy and security procedures that were mandated by federal, state, and local laws and industry standards.

129. Defendants should be compelled to provide for the benefit of Plaintiff and class members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT V
DECLARATORY RELIEF
(28 U.S.C. § 2201)
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the California Subclass)

130. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

131. An actual controversy has arisen and exists between Plaintiff and class members, on the one hand, and Defendants on the other hand, concerning the Data Breach and Defendants' failure to protect Plaintiff's and class members' PHI and PII, including with respect to the issue of whether Defendants took adequate measures to protect that information. Plaintiff and the Class are entitled to judicial determination as to whether Defendants have performed and are adhering to all data privacy obligations as required by law or otherwise to protect Plaintiff's and class members' PHI and PII from unauthorized access, disclosure, and use.

132. A judicial determination of the rights and responsibilities of the parties regarding Defendants' privacy policies and whether they failed to adequately protect PHI and PII is necessary and appropriate to determine with certainty the rights of Plaintiff and the Class, and so that there is clarity between the parties as to Defendants' data security obligations with respect to PHI and PII going forward, in view of the ongoing relationships between the parties.

COUNT VI
Violation of the California Confidentiality of Medical Information Act
Cal. Civ. Code § 56, *et seq.* ("CMIA")
(On Behalf of Plaintiff and the California Subclass)

133. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

134. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

135. Defendants are providers of healthcare within the meaning of Cal. Civ. Code § 56.05(d) because both Defendants are "contractor[s]" within the meaning of Cal. Civ. Code § 56.05(d) and/or "business[es] organized for the purpose of maintaining medical information" and/or "business[es] that offer[] software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Cal. Civ. Code §§ 56.06(a) and (b), and maintained and continue to maintain "medical information," within the meaning of Cal. Civ. Code § 56.05(j), for "patients," within the meaning of Cal. Civ. Code § 56.05(k).

136. Plaintiff and California Subclass members are "patients" within the meaning of Cal. Civ. Code § 56.05(k) and are "endanger[ed]" within the meaning of Cal. Civ. Code § 56.05(e), because Plaintiff and California Subclass members fear that disclosure of their PHI and medical information could subject them to harassment or abuse.

137. Plaintiff and California Subclass members had their PHI and medical information created, maintained, preserved, and stored on Defendants' computer networks at the time of the Data Breach.

138. Defendants, through inadequate security, allowed an unauthorized third party to gain access to Plaintiff's and other California Subclass members' PHI, medical information, and other PII without the prior written authorization required by Cal. Civ. Code § 56.10 of the CMIA.

139. Defendants violated Cal. Civ. Code § 56.101 of the CMIA by failing to maintain and preserve the confidentiality of Plaintiff's and other California Subclass members' PHI, PII, and medical information.

140. As a result of Defendants' above-described conduct, Plaintiff and California Subclass members have suffered damages from the unauthorized disclosure and release of their PHI, PII, and medical information.

141. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and California Subclass members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their medical information, (iv) statutory damages under the CMIA, (v) deprivation of the value of their medical information, for

which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

142. Plaintiff , individually and for each member of the California Subclass, seeks nominal damages of one thousand dollars ($1,000) for each violation under Cal. Civ. Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Cal. Civ. Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiff and California Subclass member, and attorneys' fees, litigation expenses and court costs, pursuant to Cal. Civ. Code § 56.35.

COUNT VII
Violations of the California Customer Records Act
Cal. Civ. Code § 1798.80, *et seq.* ("CCRA")
(On Behalf of Plaintiff and the California Subclass)

143. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

144. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

145. By failing to implement reasonable measures to protect the California Subclass's PHI and PII, Defendants violated Cal. Civ. Code § 1798.81.5.

146. In addition, by failing to promptly notify all affected California Subclass members that their PHI and PII Information had been exposed, Defendants violated Cal. Civ. Code § 1798.82.

147. As a direct or proximate result of Defendants' violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members were (and continue to be) injured and have suffered (and will continue to suffer) the damages and harms described herein.

148. In addition, by violating Cal. Civ. Code §§ 1798.81.5 and 1798.82, Defendants "may be enjoined" under Section 1798.84(e).

149. Defendants' violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82 also constitute unlawful acts or practices under the Unfair Competition Law, which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

150. Plaintiff accordingly requests that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Defendants utilize strong industry standard data security measures and file transfer software for the transfer and storage of customer data; (2) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (3) ordering that Defendants engage third party security auditors and internal personnel to run automated security monitoring; (4) ordering that Defendants

audit, test and train security personnel regarding any new or modified procedures; (5) ordering that Defendants purge, delete, and destroy in a reasonably secure manner class member data not necessary for its provisions of services; (6) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (7) ordering that Defendants, consistent with industry standard practices, evaluate all file transfer and other software, systems, or programs utilized for storage and transfer of sensitive PHI and PII for vulnerabilities to prevent threats to customers; (8) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (9) ordering Defendants to meaningfully educate their customers about the threats they face as a result of the loss of their PHI and PII to third parties, as well as the steps Defendants' customers must take to protect themselves.

151. Plaintiff further requests that the Court require Defendants to identify all of its impacted clients, and to identify and notify all members of the Class who have not yet been informed of the Data Breach, and to notify affected persons of any future data breaches by email within 24 hours of discovery of a breach or possible breach and by mail within 72 hours.

COUNT VIII
Violations of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL")
(On Behalf of Plaintiff and the California Subclass)

152. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

153. Defendants engaged in unfair and unlawful business practices in violation of the UCL.

154. Plaintiff suffered injury in fact and lost money or property as a result of Defendants' alleged violations of the UCL.

155. The acts, omissions, and conduct of Defendants as alleged herein constitute a "business practice" within the meaning of the UCL.

Unlawful Prong

156. Defendants violated the unlawful prong of the UCL by violating, without limitation, the CCRA and CMIA, as alleged above.

157. Defendants' conduct also undermines California public policy—as reflected in statutes like the California Information Practices Act, Cal. Civ. Code § 1798, et seq., the CCPA concerning consumer privacy, the CMIA concerning medical records and information, and the CCRA concerning customer records—which seek to protect customer and consumer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

Unfair Prong

158. Defendants' acts, omissions, and conduct also violate the unfair prong of the UCL because Defendants' acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and other class members. The gravity of Defendants' conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendants' legitimate business interests, other than Defendants' conduct described herein.

159. Defendants' failures to utilize, and to disclose that they do not utilize, industry standard security practices constitute an unfair business practice under the UCL. Defendants' conduct is unethical, unscrupulous, and substantially injurious to the Class. While Defendants' competitors have spent the time and money necessary to appropriately safeguard their products, service, and customer information, Defendants have not—to the detriment of their customers and to competition.

Fraudulent Prong

160. By failing to disclose that they do not enlist industry standard security practices, which rendered class members particularly vulnerable to data breaches, Defendants engaged in UCL-violative practices.

161. A reasonable consumer would not have utilized Defendants' services, and/or entrusted their PII and PHI to Defendants' clients that utilized Defendants' services, if they knew the truth about Defendants' security procedures. By withholding material information about their security practices, Defendants were able to obtain customers who provided and entrusted their PII and PHI to Defendants. Had Plaintiff known the truth

about Defendants' security procedures, Plaintiff would not have done business with the Defendants and/or their clients that utilized Defendants' services.

162. As a result of Defendants' violations of the UCL, Plaintiff and class members are entitled to injunctive relief including, but not limited to: (1) ordering that Defendants utilize strong industry standard data security measures and file transfer software for the transfer and storage of customer data; (2) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (3) ordering that Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (4) ordering that Defendants audit, test and train its security personnel regarding any new or modified procedures; (5) ordering that Defendants purge, delete, and destroy in a reasonably secure manner class member data not necessary for its provisions of services; (6) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (7) ordering that Defendants, consistent with industry standard practices, evaluate all file transfer and other software, systems, or programs utilized for storage and transfer of sensitive PII and PHI for vulnerabilities to prevent threats to customers; (8) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (9) ordering Defendants to meaningfully educate their customers about the threats they face as a result of the loss

of their PII and PHI to third parties, as well as the steps Defendants' customers must take to protect themselves.

163. As a result of Defendants' violations of the UCL, Plaintiff and class members have suffered injury in fact and lost money or property, as detailed herein. They agreed to transact business and purchase services from Defendants and/or Defendants' customers utilizing Defendants' services, or made purchases or spent money that they otherwise would not have made or spent, had they known the truth. Class members lost PHI and PII, which is their property, and privacy in that information. Class members lost money as a result of dealing with the fallout of the Data Breach, including, among other things, negative credit reports, the value of time they expended monitoring their credit and transactions, resolving fraudulent charges, and resolving issues that resulted from the fraudulent charges and replacement of cards. Plaintiff and class members are exposed to an ongoing risk of harm because their PHI and PII is not adequately protected by Defendants, and is now in the hands of criminals. Plaintiff and class members will continue to spend time, money, and resources in attempting to prevent and rectify fraud resulting from their PII and PHI being exposed by Defendants.

164. Plaintiff requests that the Court issue sufficient equitable relief to restore class members to the position they would have been in had Defendants not engaged in violations of the UCL, including by ordering restitution of all funds that Defendants may have acquired from Plaintiff and class members as a result of those violations.

COUNT IX
Violation of the California Constitution, art. 1, § 1
(On Behalf of Plaintiff and the California Subclass)

165. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

166. Plaintiff and California Subclass members had a reasonable expectation of privacy in their PHI and PII that Defendants disclosed without authorization.

167. By failing to keep Plaintiff's and California Subclass members' PII and PHI safe, and by disclosing said information to unauthorized parties for unauthorized use, Defendants invaded Plaintiff's and California Subclass members' privacy by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. violating their right to privacy under California Constitution, Article 1, Section 1, through the improper use of private information properly obtained for a specific purpose for another purpose, or the disclosure of it to some third party.

168. Defendants invaded Plaintiff's and California Subclass members' right to privacy and intruded into Plaintiff's and California Subclass members' private affairs by disclosing their PII and PHI to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

169. Plaintiff and California Subclass members have a reasonable expectation of privacy and a constitutionally protected privacy interest in their confidential PHI and PII.

170. As a proximate result of these unauthorized disclosures, Plaintiff's and California Subclass members' reasonable expectations of privacy in their PII and PHI were unduly frustrated and thwarted, and their constitutional right to privacy was violated. Defendants' conduct amounted to a serious invasion of Plaintiff's and California Subclass members' protected privacy interests.

171. In failing to protect Plaintiff's and California Subclass members' PII and PHI, and in disclosing the same, Defendants acted with malice and oppression and in conscious disregard of Plaintiff's and California Subclass members' constitutional rights to have such information kept confidential and private.

172. Plaintiff and California Subclass members seek compensatory and punitive damages, injunctive relief, restitution, attorneys' fees and costs, and all other damages available under this Count.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Class, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as Class Representative and undersigned counsel as Class Counsel;

B. Award Plaintiff and the Class actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that class members have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

D. Award Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and the Class such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: August 2, 2023

Respectfully submitted,

By: */s/ E. Michelle Drake*

E. Michelle Drake (Bar No. 0387366)
BERGER MONTAGUE, PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
Email: emdrake@bm.net

Mark B. DeSanto (*Pro Hac Vice* forthcoming)
BERGER MONTAGUE, PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4604
Email: mdesanto@bm.net

Attorneys for Plaintiff